ISBN: 1646-8929

IET Working Papers Series
No. WPS01/2016

David Duarte
(email: dj.duarte@campus.fct.unl.pt)
Tiago Mealha
(email: t.mealha@campus.fct.unl.pt)

Introdução à "Deep Web"

IET/CICS.NOVA
Innovation and Technology Studies pole at FCT-UNL
Centro Interdisciplinar de Ciências Sociais
Faculdade de Ciências e Tecnologia
Universidade Nova de Lisboa
Monte de Caparica
Portugal

Introdução à DEEP WEB[1]

David Duarte
(email: dj.duarte@campus.fct.unl.pt)

Tiago Mealha
(email: t.mealha@campus.fct.unl.pt)

1ª versão: 17 de Dezembro 2015

2ª versão: 13 de Março 2016

Resumo

A *Deep Web* é a parte da *Internet* que não se encontra registada, não sendo possível acedê-la pelos motores de busca tradicionais. É preciso recorrer a *software* que permitem preservar a identidade dos utilizadores, como por exemplo o *Tor*, sendo este o mais conhecido. Conceitos como *Deep Web*, *Darknet* e *Dark Web* são erradamente confundidos, questão que este artigo trata de elucidar.

Outra temática que se aborda é a conotação negativa muitas vezes atribuída ao fenómeno da *Deep Web*. Por salvaguardar o anonimato dos seus utilizadores, muitas pessoas aproveitam para praticar negócios ilícitos, como transação de drogas, armas, etc. É aqui que chegamos ao centro do debate: por um lado o *Tor* permite, entre outras coisas, assegurar a privacidade das comunicações entre utilizadores e visualizar artigos e *blogs* que não se encontram na *Surface Web*; por outro lado o anonimato serve de ferramenta para que ocorra a prática de atividades ilícitas.

Existe uma linha muito ténue que separa a esfera pública da esfera privada. O *Tor* permite reforçar a segurança ao utilizar a *Internet*. Cabe ao bom senso de cada um a forma como utiliza as ferramentas ao seu dispor.

Palavras-chave: Deep Web, Internet, Tor, privacidade, segurança

[1] Trabalho baseado no relatório para a disciplina "Sociologia das Novas Tecnologias de Informação" no âmbito do Mestrado Integrado de Engenharia e Gestão Industrial, da Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa em 2015-16. O trabalho foi orientado pelo Prof. António Brandão Moniz do Departamento de Ciências Sociais Aplicadas (DCSA) na mesma Faculdade.

Abstract

Deep Web is the part of the Internet that is not indexed, not being possible to access through the traditional web search engines. It is necessary to use software that preserves the identity of the users, for instance, Tor, which is the most well-known. Concepts such as Deep Web, Darknet and Dark Web are mistakenly confused but this article will clarify it.

Another theme approached is the negative connotation that is usually assigned to the Deep Web phenomenon. Because protects the users' anonymity, a lot of people take advantage of it to commit illegal businesses, for example drugs and weapons transactions. We reach to the central question of our debate: on the one hand, the Tor software preserves the intimacy of the users' communications and allows the consult of several articles and blogs that does not exist on the Surface Web; on the other hand the anonymity serves as a tool for the practice of illegal activities.

There is a very thin line that separates public space and private space. Tor software reinforces the security of using the Internet. The application that people utilize it is up to them.

Keywords: Deep Web, Internet, Tor, privacy, security

JEL codes: G02, K49, O34

Conteúdo

1. Introdução e motivação

O presente relatório tem como objetivo apresentar um tema fraturante da sociedade moderna, e que se enquadra no tema da sociologia das novas tecnologias de informação. Para além de apresentar este tema, pretende-se também vincar o debate entre diferentes opiniões, bem como mostrar até que ponto as mesmas interferem com a sociedade.

A *Internet* abriu portas a toda uma nova era para as tecnologias de informação, para o modo como as pessoas têm acesso à informação e como se conectam entre elas. As pessoas estão agora à distância de um *click*, e a informação está facilmente ao alcance. Trouxe comodidade, pois a velocidade com que se tem acesso ao conhecimento não tem precedente, para além de estar facilmente acessível. Em qualquer cidade é possível encontrar redes *wifi* com as quais acedemos à *Internet*, não só através de computadores, mas também de *smartphones*. Estamos portanto a presenciar o momento da revolução das novas tecnologias de informação.

Tudo começou com o telégrafo, o primeiro dispositivo que permitiu a troca de informação e comunicação à distância. Hoje em dia, apesar desta tecnologia estar já ultrapassada, os princípios e motivações são os mesmos, tal como os riscos.

No futuro, prevê-se que as pessoas vivam em casas inteligentes, nas quais a acessibilidade, comodidade e segurança são os conceitos valorizados. No entanto, existe um preço a pagar: as casas inteligentes serão com certeza cómodas e com elevados níveis de acessibilidade, mas serão totalmente seguras? Para que se possa usufruir das funcionalidades das casas inteligentes, é necessário que a base de dados da casa seja abastecida com as rotinas dos seus moradores. A casa desligará as luzes à hora que o morador tenha por hábito deitar-se para dormir e ligará quando por hábito o morador acorda. Este é apenas um dos vários exemplos de como a casa reconhece as rotinas, armazenando-as e tornando-as úteis em prol do morador. Em suma, estes dados são armazenados por dispositivos eletrónicos que conseguem mesmo reconhecer padrões e atuar em conformidade (inteligência artificial), o que acontecerá se toda esta informação estiver na posse das pessoas erradas?

Ao longo do relatório serão apresentados diversos casos que expõem a dicotomia que origina as perguntas: até que ponto estamos dispostos a ceder a nossa privacidade? Qual o valor da nossa privacidade?

2. Conceitos básicos

Neste capítulo serão apresentadas breves noções de alguns conceitos básicos, que se entendem ser relevantes para a melhor compreensão do tema a ser tratado. Trata-se de conceitos que serão frequentemente mencionados, e cujas definições poderão ser frequentemente confundidas. Assim, torna-se útil clarificá-los para mais tarde serem devidamente contextualizados. Ainda assim, neste mesmo capítulo, sempre que pertinente, uma breve contextualização ao tema será feita.

2.1 Privacidade

Privacidade é um conceito que diz respeito ao direito reservado de informações e dados pessoais de cada indivíduo. Refere-se ao direito que cada um tem de controlar a sua própria exposição e de dispor a sua informação para o conhecimento público. Este conceito diz ainda respeito ao direito ao anonimato numa sociedade.

A privacidade é um direito incluído na *Declaração Universal dos Direitos Humanos* formulada pelas Nações Unidas, citando: "*Ninguém deverá ser submetido a interferências arbitrárias na sua vida privada, família, domicílio ou correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques todas as pessoas têm o direito à proteção da lei.*"

No contexto em questão, convém ainda distinguir o conceito de privacidade digital, termo esse desenvolvido mais recentemente com o aparecimento de novas tecnologias de informação, e que diz respeito ao direito à mesma na Internet. A atual arquitetura da *Internet* permite que cada pessoa possa aceder e formular políticas de privacidade, e os utilizadores têm o direito e dever de estarem familiarizados com as mesmas.

No entanto, ao contrário da "vida real", sente-se alguma ausência de leis reguladoras consolidadas em relação à privacidade digital com vários omissos. É comum nos dias de hoje a violação desse direito, sobretudo em redes sociais e outros *sites* que permitam o compartilhamento de conteúdos e opiniões.

Uma das grandes áreas de pesquisa no que toca à *Internet* prende-se com a busca de soluções para garantir a privacidade digital e proteção de dados. Esta área torna-se extremamente relevante uma vez que hoje em dia até é possível efetuar transações monetárias. "Até que ponto a privacidade está a ser violada?" É ainda uma questão polémica e que divide a opinião pública, pois muitos utilizadores da Internet têm uma curta noção do que realmente acontece às informações partilhadas e como se processa esse fluxo de informação. Exemplos: a venda de informação legal de dados compartilhados nas redes sociais sem aviso prévio, e o sistema de publicidade *online*.

2.2 Tecnologias de informação

As Tecnologias de Informação (TI) definem-se como todas as soluções oferecidas por recursos eletrónicos e computacionais que permitem a transferência e armazenamento de dados e informação processada. Apesar das múltiplas áreas onde as TI têm clara influência, o contexto da informática é um dos quais as TI têm maior influência, pois são úteis quer em segurança, organização e arquitetura da *Internet*, *download* e *upload* de conteúdos e classificação. As TI tiveram um papel fulcral no desenvolvimento de programas de processamento de texto, sistemas de armazenamento de dados computacionais, transferências e consultas na *Internet*. As TI têm ainda um papel muito importante no que toca à preservação da liberdade e privacidade digital, ou por outro lado, a violação das mesmas, dependendo do uso que lhes são dadas.

São ainda as TI as responsáveis pelo aperfeiçoamento dos sistemas de inteligência artificial, que permitem que dispositivos eletrónicos armazenem dados e reconheçam padrões e tendências nos mesmos tomando por si só decisões em conformidade.

Os países com maior investimento em TI são os Estados Unidos da América, Suécia, Dinamarca e Singapura.

2.3 Internet

A *Internet* é um sistema de conexão entre computadores, que permite a comunicação entre eles, bem como a consulta e partilha de informação. Trata-se de uma rede de comunicações que abrangem a esfera pública, privada, académica, laboral e governamental, conectadas por ligações fixas ou sem-fios.

A consulta e partilha de informação podem ser feitas na *World Wide Web* (www), mais familiarmente denominada *Web*, em que se pode aceder através da Internet. A Web é um espaço aberto onde documentos e outros recursos estão registados e identificados por endereços eletrónicos. Para "navegar" num determinado *website*, basta escrever o exato endereço eletrónico ou então procurar nos motores de busca, como por exemplo o *Google*.

A *Internet* divide-se em dois segmentos: a *Surface Web*, que corresponde à parte da *Internet* que está registada e que é facilmente acedida através dos motores de busca, e a *Deep Web*, que se baseia no conteúdo da *Internet* que não está registado e que não pode ser consultado da maneira convencional.

2.3.1 *Surface Web*

Como foi referido anteriormente, a *Surface Web* diz respeito aos *websites* que estão registados e que podem ser acedidos através dos motores de busca. Estes constroem uma espécie de histórico de dados, através de programas denominados *Web Crawlers*, que começam com uma lista de páginas de Internet conhecidas, tais como o *Facebook* e *Youtube*. Esse programa pega numa cópia de cada página e regista-a, guardando informações importantes que irão permitir que a página seja mais tarde recuperada. Todos os endereços eletrónicos de novas páginas são registados. O conjunto dessas páginas constitui a *Surface Web*. Estima-se que, atualmente, existam cerca de 15 biliões de sites indexados.

2.3.2 *Deep Web*

Recentemente, este conceito tem suscitado o interesse das pessoas devido ao escândalo que assolou a sociedade: o caso de Ross Ulbritch, um jovem norte-americano que geria um *site* de compra e venda de drogas, de nome "*Silk Road*". Estima-se que Ross tenha gerado mais de 200 milhões de euros nas transações efetuadas por essa plataforma. Mas existem vários conceitos que são erradamente confundidos pelas pessoas. Ao longo do relatório, esses conceitos serão claramente explicados. De seguida, irá ser dado a conhecer o fenómeno da *Deep Web*.

A *Deep Web, Deep Net, Invisible Web* ou *Hidden Web* são termos que se referem ao conteúdo da *Internet* que não se encontra registado pelos tradicionais motores de busca. No ano de 2000, Michael k. Bergman afirmou que pesquisar na Internet pode ser como pescar na superfície de um oceano- um grande peixe pode ser apanhada na rede contudo, existe uma imensidão de peixes mais ricos que se encontram nas profundezas e, consequentemente não foram pescados. A maior parte da informação na *Internet* está tão profunda que os motores de busca tradicionais não a reconhece. A seguinte imagem ilustra a diferença de proporções entre a *Surface Web* e a *Deep Web*:

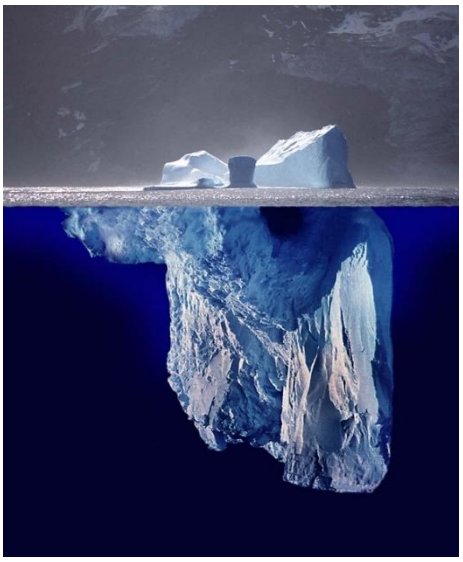

Imagem 1- Diferença entre *Surface* e *Deep Web*

É impossível medir o tamanho da *Deep Web*. Dados anteriores apontam para 400 ou 500 vezes superior ao da *Surface Web*. E a tendência é de aumentar exponencialmente. Ao longo do tempo, informáticos têm explorado o quão profunda a *Deep Web* poderia ser localizada de uma forma automática, tendo então desenvolvido um *software* de pesquisa de informação da *Deep Web*, por outras palavras uma *Darknet*, chamado *Tor*, uma ferramenta que permite preservar o anonimato do utilizador, requisito imprescindível para aceder à *Deep Web*. *Tor* é um conceito o qual será mais tarde abordado detalhadamente no relatório.

De momento, existe uma conotação negativa sempre que se ouve falar da *Deep Web*. O risco de aceder a esta parte da Internet resume-se à intenção que o utilizador tem em utilizá-la. Naturalmente que, por ser criptografada e anónima, permite a certos utilizadores praticar certa atividade ilícita.

2.4- Darknet

A *Darknet* é uma rede de ligações que só poderá ser consultada com o uso de *softwares* específicos. Existem 2 tipos de *Darknet*: a ligação *friend-to-friend*, onde os utilizadores comunicam com pessoas que conhecem, e onde *passwords* e assinaturas digitais podem ser utilizadas para autentificação, e o *software* anónimo *Tor*, que preserva a identidade dos utilizadores. De um modo geral, a *Darknet* é utilizada por:

- Cidadãos que querem proteger a sua privacidade;
- Proteger dissidentes por represálias políticas;
- *Whistleblowers*;
- Utilizadores que cometem crimes informáticos (*hacking*);
- Compradores e vendedores de negócios ilícitos;
- Partilha de ficheiros (pornografia, ficheiros confidenciais, *software* ilegal, etc.).

Toda a *Darknet* requer *software* específico para ser acedida, como o *Tor*, que pode ser instalado através do *browser* do *Tor* ou, em alternativa, através de um *proxy* (um servidor intermediário) que desempenha as mesmas funções. Tal como o *Tor*, existem outros *softwares* que executam a mesma tarefa, como por exemplo o *I2P*, *Freenet* e o *RetroShare*.

2.5- Dark Web

Dentro da *Deep Web*, existem *websites* não registados e que só podem ser consultados com o uso de uma *Darknet*, como por exemplo o *Tor*, constituindo assim a *Dark Web*. Um estudo feito pela Universidade de Portsmouth, no Reino Unido, em dezembro de 2014, chegou à conclusão que o tipo de conteúdo mais visitado na *Dark Web* é pornografia infantil, logo seguida por mercados negros. São igualmente requisitados *sites* de divulgação de segredos de Estado (*WikiLeaks*) e fóruns de política, bem como páginas sobre fraude informática e *Bitcoins*, este último iremos abordar mais tarde. De seguida, estão representadas as estatísticas, em percentagem, da quantidade de *websites* existentes na *Dark Web* por categoria:

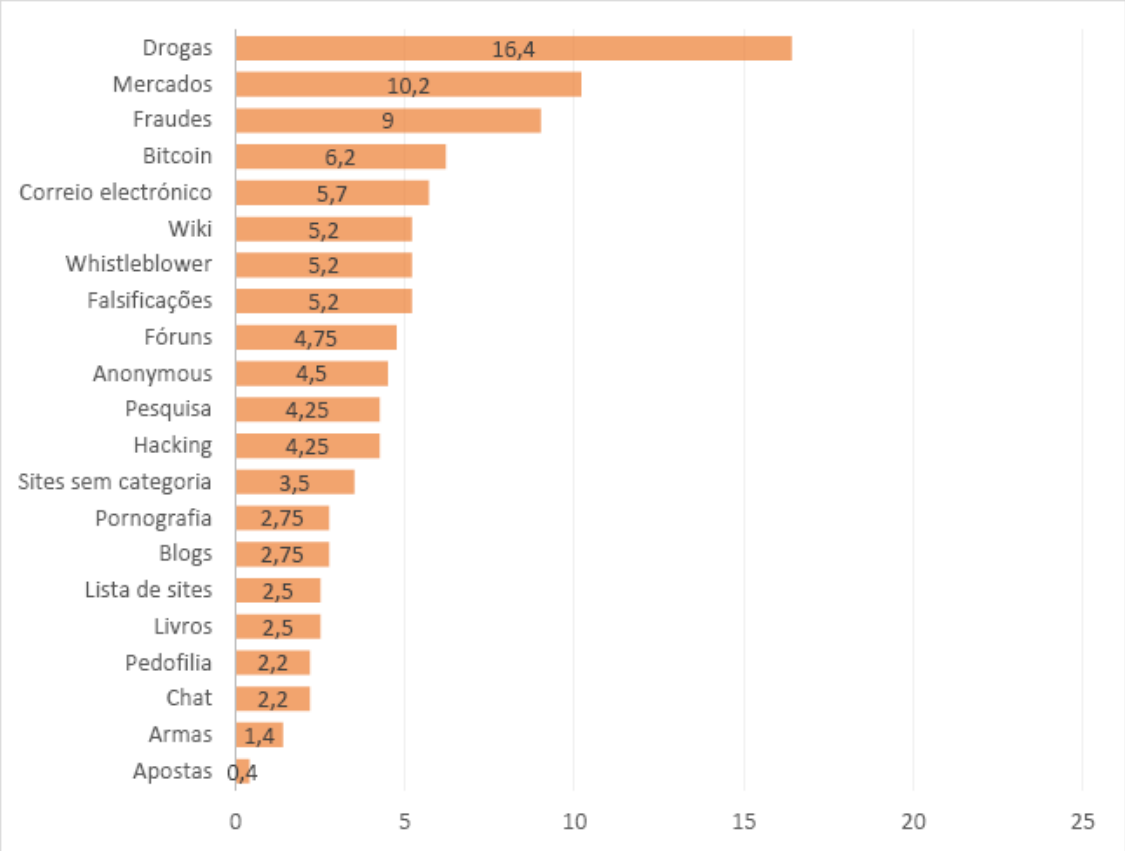

Gráfico 1- Quantidade de *websites* por categoria (%)

Como é fácil de se observar, praticamente 25% do conteúdo da *Dark Web* resume-se a *sites* de compra e venda de drogas e outros mercados ilícitos. Desde que veio a público o escândalo da plataforma *Silk Road*, as autoridades reforçaram a vigilância a este tipo de atividade.

Hacking também é muito popular. Muitos *hackers* vendem os seus serviços, como obter *passwords* ou infecta computadores com vírus, em troca de avultadas somas de dinheiro. Fraudes e falsificações fazem igualmente parte das categorias com o maior número de *websites*.

Existem relatos de pessoas que visitaram *sites* macabros na *Dark Web* onde assassinos e criminosos trocavam experiências pessoais dos crimes cometidos. Há quem diga que ocorrem sessões de homicídios em direto, em que os assassinos recebem donativos dos utilizadores que queiram assistir à cena. A 25 de junho de 2015, começou a circular no *Youtube* um vídeo de um videojogo de nome "*Sad Satan*" que se acredita que foi adquirido e só pode ser jogado na *Dark Web*.

Embora muito conteúdo da *Dark Web* seja inofensivo, o governo está preocupado com a atividade criminal praticada nesse espaço. Novos *sites* como o *DeepDotWeb* e *All Things Vice* revelam informações sobre sites e serviços da *Dark Web*. O *Hidden Wiki* é um espaço em que estão disponíveis *links* de websites das categorias anteriormente

mencionadas. Outros *sites* bastante conhecidos como o *Youtube*, *Twitter* e *Reddit* também revelam informações acerca do que esperar no lado mais obscuro da Internet.

2.6 Criptografia

A criptografia refere-se ao estudo das técnicas de transformação e codificação em informação na sua forma original legível em alterada e ilegível, com o intuito da mensagem ser apenas compreensível pelo emissor (autor da mensagem) e destinatário. Ambos emissor e destinatário detêm o código para descodificar ou desencriptar a mensagem codificada ou encriptada. Criptografia diz respeito a um ramo das ciências matemáticas chamado Criptologia, visto que este conjunto de técnicas utiliza fundamentos e bases matemáticas muito atuais. A criptografia moderna estuda os algoritmos criptográficos a serem implementados em computação e informática. A criptografia obedece a quatro princípios fundamentais, a saber:

1- Confidencialidade: apenas o destinatário deverá ter acesso a chave que decifra a mensagem encriptada;

2- Integridade: o destinatário deverá ter a capacidade de saber se a mensagem sofreu alterações durante a transmissão;

3- Autenticidade: o destinatário deverá conseguir identificar o emissor da mensagem;

4- Irretratabilidade: o emissor não poderá conseguir negar o autor da mensagem (emissor).

A criptografia é portanto uma ferramenta que se revela extremamente útil na preservação da privacidade *online*.

2.7 Dark Wallet (Bitcoins)

Bitcoin é uma moeda virtual utilizada para efetuar transações anónimas entre pessoas por via digital. Inventada e partilhada em 2009 pelo japonês Satoshi Nakamoto, a *Bitcoin* é uma moeda encriptada que todas as pessoas podem adquirir em troca de dinheiro, produtos ou serviços. O número de pessoas a utilizar este método tem vindo a crescer largamente e uma das razões para tal é o facto das taxas de pagamento serem de 2 a 3 % mais baratas do que o pagamento por cartão de crédito. Ao contrário do método tradicional, as taxas são suportadas pelo comprador, e não pelo vendedor.

Muitas organizações têm vindo a aderir a esta carteira virtual, sendo que estas começaram recentemente a aceitar donativos em *Bitcoins*, cujo símbolo é representado por BTC ou ฿. Como exemplo destas organizações tem-se a *Greenpeace*, a *Mozilla Foundation* e a Universidade de Nicósia. Desde setembro de 2014 que a *PayPa*l permite receber pagamentos em *Bitcoins*.

Mas como funciona esta nova moeda? Trata-se de dinheiro virtual que circula eletronicamente e que é controlado por um algoritmo. Uma transação entre duas pessoas procede-se da seguinte maneira: as duas partes têm de assinar uma chave encriptada, indicando que estão de acordo em relação aos moldes da transação. Consequentemente, um registo eletrónico dessa transação é efetuado e é enviado para o histórico de transações - o *Block Chain*. Este histórico é distribuído a cada utilizador e é extremamente complicado de ser rastreado.

Bitcoins podem ser adquiridas diretamente a pessoas, através de máquinas multibanco ou em leilões. Não existe uma tabela fixa de conversão de *Bitcoins* mas estima-se que o seu valor é 7 vezes superior ao ouro e 18 vezes superior ao *dólar* americano. A definição de *Bitcoin* não é consensual, sendo que nalguns países, como a Rússia, o Vietname e o Equador, é proibida a sua circulação.

Devido ao seu formato anónimo, a *Bitcoin* é a moeda utilizada para as transações efetuadas na *Dark Web*, nomeadamente na famosa plataforma de compra e venda de drogas, a *Silk Road*, bem como para aquisição de material ilegal como pornografia infantil, armas, assassinos, etc. Estes factos têm suscitado críticas à utilização desta moeda por parte do *FBI*.

3. Limites da privacidade online

Quais os verdadeiros limites do conceito de privacidade, no contexto cibernético, é uma questão que foi levantada quando os utilizadores da *Internet* em geral, se aperceberam das consequências negativas que a *Internet* promovia.

Tendo em consideração que, sempre que um utilizador se encontra *online*, todos os dados que por ele são criados, desde *sites* visitados, mensagens trocadas, *upload* e *download* de conteúdo, são registados pelos *softwares* de leitura de dados *online*, estes, providos de tecnologia de inteligência artificial de ponta, são capazes de proceder a análise de dados padronizados, e, deste modo identificar tendências que, em informação produzida, são associados a rotinas de utilização da *Internet*. Os dados de utilização da *Internet* facilmente identificam as rotinas do utilizador, e esta informação é de extrema importância para as empresas que pretendam conhecer o seu *target*, e tomar medidas estratégicas nesse sentido. Como tal, os domínios *online* que possuem este tipo de informação, aperceberam-se do valor que tinham para as empresas e começaram a comercializar este tipo de informação.

Os utilizadores da *Internet* aperceberam-se então que a informação acerca deles próprios estava a ser trocada e que um novo negócio nascera, sem o seu consentimento ou noção de tal facto. Hoje em dia, muitas são as empresas que, para publicitar o seu produto ao cliente, recorrem e pagam por esta informação, com o intuito de produzir conteúdo publicitário personalizado aos clientes, e assim, incitar à procura. Tal facto justifica o porquê da publicidade *online* dizer sempre respeito ao utilizador em questão. Os utilizadores da *Internet* têm assim o seu espaço privado invadido sem permissão, constando assim uma violação do conceito de privacidade anteriormente enunciado. No entanto, o conceito de privacidade no contexto digital não é totalmente semelhante no que toca à aplicação do conceito global de privacidade. Como foi também mencionado, devido à presença de omissos na aplicação do código jurídico neste contexto, a execução das leis não ocorrem tão eficaz e eficientemente como se pretende, tornado a situação em causa recorrente.

Os serviços de segurança nacional utilizam também a informação acerca da "pegada *online*" para controlo do crime nas ruas, executar medidas estratégicas de segurança, bem como outras métricas que possam ser interessantes para avaliar o comportamento dos indivíduos.

Desta forma, surge então a pergunta "Até onde estamos dispostos a ceder a nossa privacidade?" que remete a dicotomia entre privacidade e segurança. A situação torna difícil distinguir onde termina o mundo exterior e começa o espaço privado, e identificar que informações pessoais estaremos nós dispostos a partilhar.

Um dos acontecimentos que alertou os utilizador para a existência destes problemas que se geram, foram as questões levantadas por Edward Snowden quanto à segurança dos sistemas primários de análise de dados *online*. Visto que são estes os primeiros recetores do fluxo de informação, o que aconteceria se tal informação fosse intercetada ou estivesse ao acesso de mãos erradas? Passa-se que, na verdade, a própria tecnologia de sistemas de cabos de transmissão de fibra ótica muito utilizada neste contexto apresenta pontos fracos.

Umas das respostas encontradas foi a criação de uma espécie de "anonimato" quando se utiliza a *Internet*. O utilizador deixaria de criar a dita "pegada *online"* se não fosse possível identificar o seu IP ao longo da sua utilização, evitando assim que os dados por ele produzidos nunca chegassem a existir, resultando em informação acerca dos seus hábitos de consulta na *Internet*.

4. Tor

Trata-se do requisito necessário para aceder ao lado mais obscuro da *Internet*. Sem este, ou um *software* similar, não é possível visualizar os conteúdos da *Deep Web*. O *Tor* (*The Onion Route)* é um *software* gratuito que permite comunicar de forma anónima. Isto é possível graças a um grupo de voluntários que funcionam como servidores, promovendo a privacidade e a segurança dos utilizadores. Para além de salvaguardar a identidade das pessoas que o utilizem, o *Tor* também permite aceder ao conteúdo da *Internet* que se encontra normalmente bloqueado na denominada *Surface Web*. A forma de atuar do *Tor*, que irá ser explicado em breve, possibilita aos utilizadores criar *sites* e outros serviços sem revelar a localização fixa do *site*. A quantidade de pessoas que utilizam esta ferramenta é o que está por trás da sua eficiência. O *Tor* esconde um utilizador entre todos os utilizadores, portanto quanto maior for o número de pessoas a usar o *software*, maior será a proteção.

Mas porquê utilizar o *Tor*? Porque protege os utilizadores da vigilância na *Internet,* mais conhecida como a "análise de tráfego". Esta deteta e regista as comunicações e as identidades das pessoas. Sabendo a fonte e o destino das comunicações, permite que desconhecidos tenham conhecimento de interesses e comportamentos dos utilizadores. Por exemplo, se uma pessoa está a viajar e conecta-se a uma ligação sem-fios para consultar o seu correio eletrónico, pode, inadvertidamente, revelar informações como a sua morada e dados pessoais a todos aqueles que vigiam essa ligação, mesmo que esta esteja encriptada.

Como funciona a "análise de tráfego"? A transmissão de dados pela *Internet* é composta por duas partes: os dados em si e uma rede por onde vão passar os dados. Estes podem ser qualquer coisa que se queira enviar, como um *email*, o endereço de um *site* ou até uma música. Mesmo que os dados estejam encriptados, a "análise de tráfego" revela uma grande parte do tipo de comunicação que está a ser realizado, bem como o seu conteúdo. Isto porque se foca na análise da rede por onde vão passar os dados, conseguindo ler a fonte, destino, tamanho e o tempo desses mesmos dados. O problema-base reside no facto das informações poderem ser lidas através da observação da rede de transmissão de dados. Ainda mais problemático se torna quando servidores e informáticos estão autorizados para tal. Existe uma outra forma de analisar o tráfego, através de técnicas sofisticadas de informática que observa as comunicações das pessoas e organizações. Nem a encriptação impede estes ataques, visto que a encriptação apenas codifica o conteúdo das mensagens então a rede de transmissão dos dados.

O *Tor* funciona da seguinte maneira: os dados dos utilizadores são encriptados e transferidos entre vários computadores voluntários, os chamados *Relay Computers*. Ao passar de computador para computador, uma parte da encriptação é removida e é indicado para que computador os dados transferidos devem ser enviados, e por aí adiante. Assim que chegar ao computador final, os dados são decriptados e o IP do utilizador está escondido. Um esquema simples do que foi agora mencionado pode ser observado:

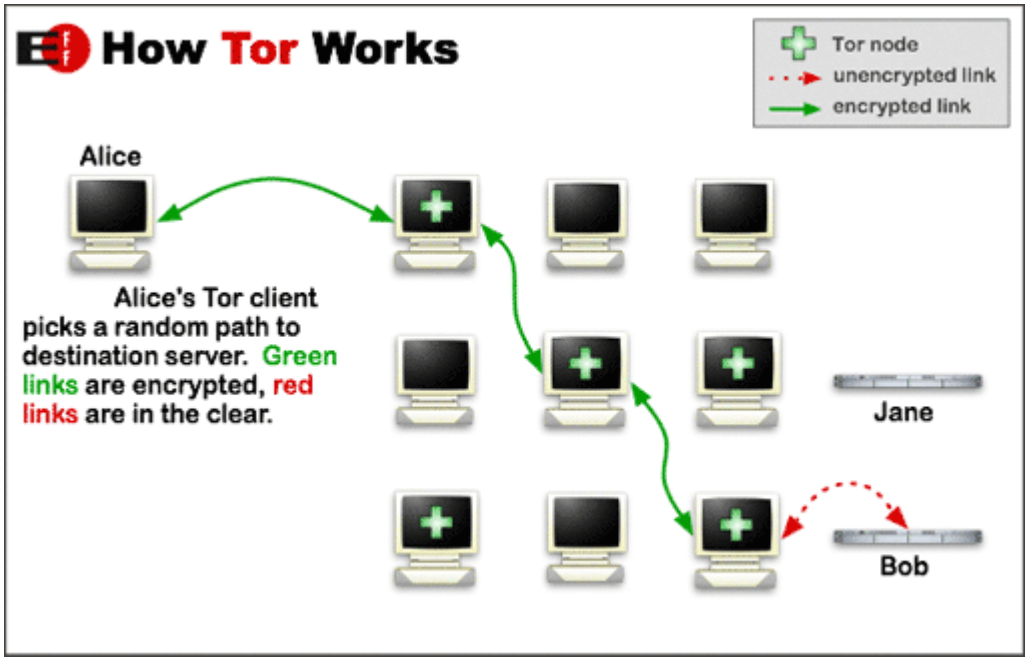

Imagem 2- Funcionamento do *Tor*

É importante conhecer um pouco da história de como nasceu o *Tor*. No final dos anos 70, na Califórnia, o criptógrafo David Chaum apercebeu-se dos perigos decorrentes da comunicação via *Internet*, nomeadamente o controlo dos dados pessoais dos utilizadores. Chaum queria resolver este problema através da encriptação das mensagens e criando uma rede anónima em que os dados eram transferidos entre vários computadores, um pouco como o *Tor* opera atualmente. Contudo, o seu projeto não passou do rascunho, visto que a comunicação pela *Internet* restringia-se na altura apenas a técnicos e académicos. Anos mais tarde, a Marinha norte-americana apercebeu-se da importância de salvaguardar as suas informações e contrata uma equipa de especialistas, liderada por Paul Syverson, para desenvolver um programa com esse fim. Inspirado pelas ideias de David Chaum, Syverson e a sua equipa inventam em 2002, o *software Tor*, que funciona como um motor de pesquisa como o *Google*.

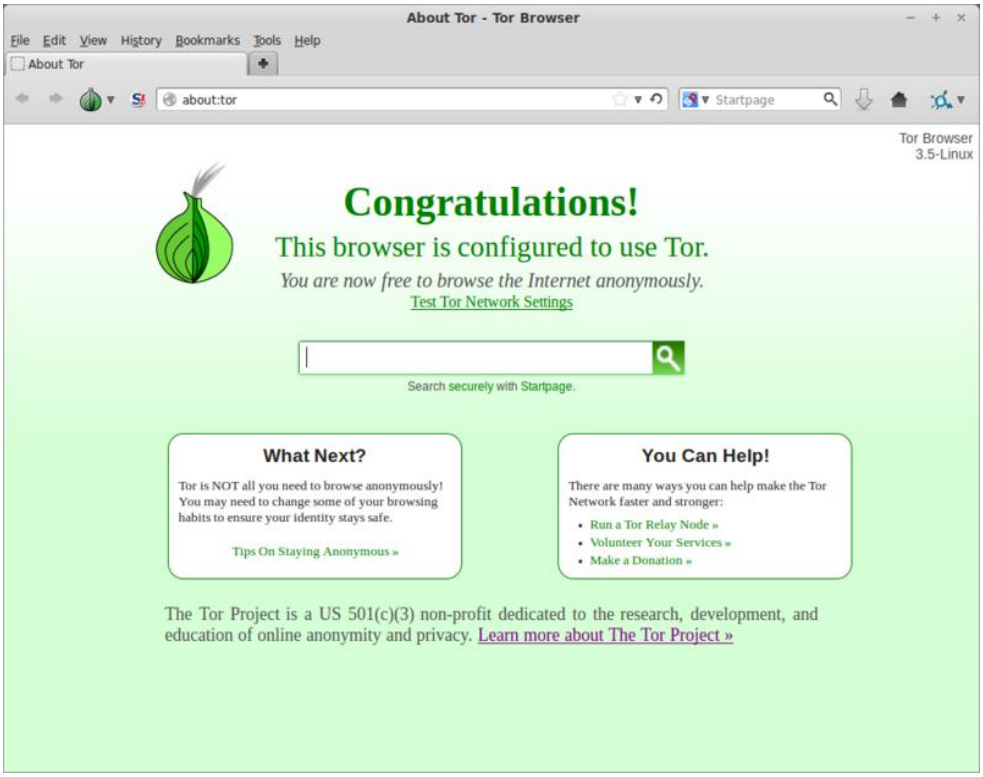

Imagem 3- *Tor*

Em 2005, este é entregue a uma organização sem fins-lucrativos. Jacob Appelbaum, jornalista e *hacker*, viaja pelo mundo para promover o uso do *Tor* e recrutar o maior número de voluntários possível para que se tornem *Relay Computers*, contribuindo para o reforço do anonimato desta ferramenta.

Nos dias de hoje, o *Tor* é mundialmente utilizado por todo o tipo de pessoas. Jornalistas usam-no para comunicar de forma segura com *whistleblowers* e dissidentes. Organizações não-governamentais utilizam para permitir que os seus trabalhadores possam aceder a *sites* dos seus países de origem enquanto se encontram no estrangeiro. Muitos ativistas também o utilizam, principalmente no Médio-Oriente, para conspirar contra o governo local. A própria Marinha norte-americana desenvolve projetos secretos através do *Tor*. Todavia, nem todos os utilizadores aplicam o *software* com inocentes intenções. O *Tor* tornou-se na principal arma de criminosos que refugiam-se nesta ferramenta para praticar atividades ilícitas, como a transação de drogas e armas, partilha de pornografia, contratação de serviços de assassinos, *hacking*, e muitos outros propósitos. Por estas razões, a Segurança Nacional Americana tem vindo a combater o *Tor*, através de ataques informáticos, mas sem sucesso. A imagem seguinte ilustra as regiões que mais utilizam este *software*.

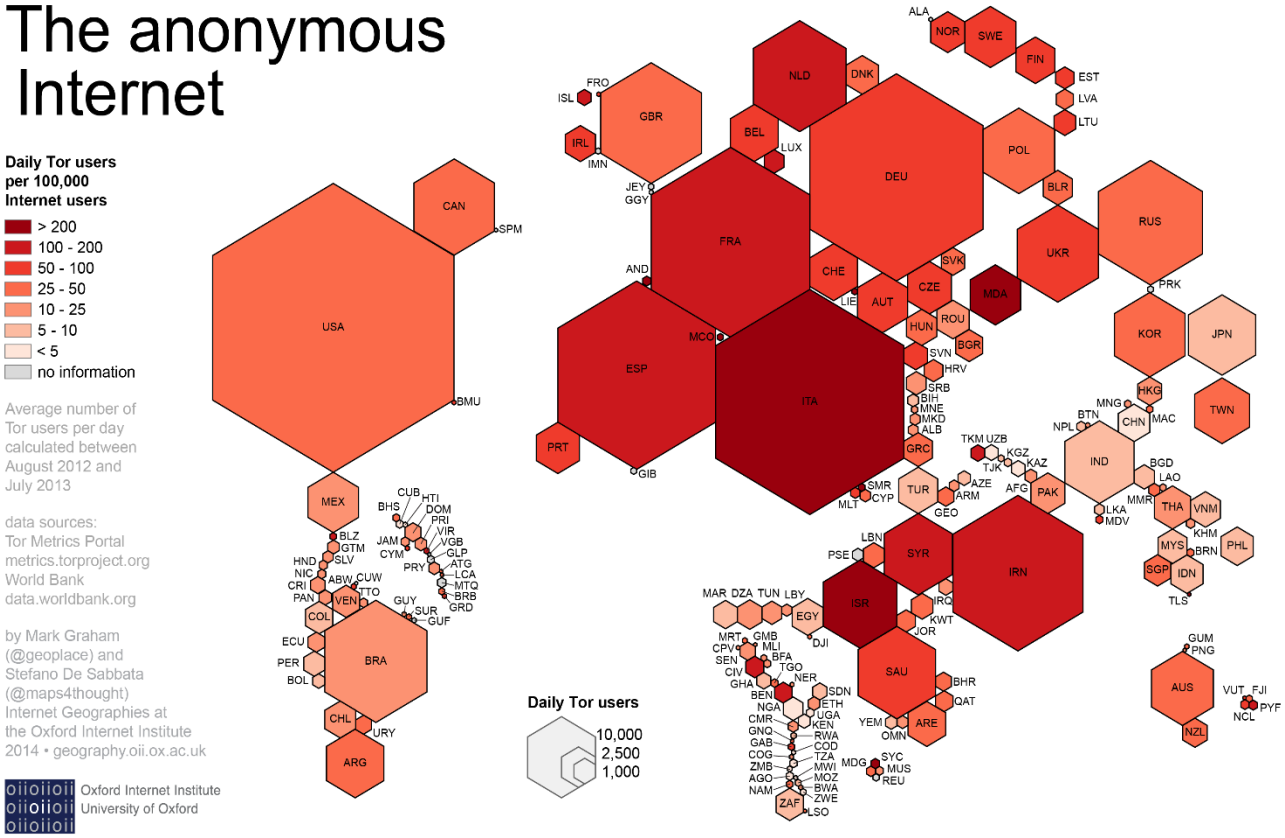

Imagem 4- Regiões do Mundo que mais utilizam o *Tor*

O *Tor* em si não resolve todos os problemas de defesa da privacidade dos seus utilizadores. Concentra-se apenas na proteção da transmissão de dados. É necessário utilizar um *software* de suporte muito específico caso as pessoas não pretendam que os *sites* que visitem verifiquem os seus dados pessoais. Quem utiliza esta ferramenta, tem de ter o cuidado de não revelar mais do que o necessário.

4.1 Lado positivo (casos)

O *Tor* é *software* que, devido às suas particularidades, especialmente proporcionar o anonimato na *Internet* e acesso à *Deep Web*, oferece a oportunidade de muitos utilizadores fazerem um uso extremamente positivo. Neste capítulo serão apresentados dois casos que simbolizam o lado positivo do *Tor* e da *Deep Web*.

4.1.1 Ativismo online

O *Tor* permite o anonimato e o acesso ao vasto conteúdo da *Deep Web*. Trata-se portanto de uma oportunidade dos utilizadores circularem na *Internet* sem deixar a sua "pegada *online"*. Não deixar a tal "pegada *online*" significa que nenhuma entidade reguladora, como os governos, consiga rastrear o percurso de um utilizador, a acrescentar a este facto, existem ainda governos de vários países, nomeadamente alguns países asiáticos como a China e o Tibete, e outros do Médio-Oriente, como o Irão e a Síria, que utilizam mecanismos de censura na *Internet*. Muitos dos países que censuram a *Internet* são países que se encontram em guerras civis e conflitos sociais, acontecimentos onde tipicamente atrocidades humanas são cometidas, tais como como violações dos direitos humanos. Estes países censuram muita da informação que é produzida diretamente nas suas fontes, sendo a *Internet* um dos mais importantes veículos de disseminação de informação. A censura chegou mesmo até à *Internet*, não permitindo que algumas situações e movimentos fossem proporcionados.

Reem Al Assil, ativista síria, tomou conhecimento das funcionalidades do *Tor* e apercebeu-se de como utiliza-las a seu favor. O seu trabalho voluntarioso como ativista neste país era gravemente interferido pelas frequentes ameaças do governo sírio e das tentativas de censura. Através do anonimato *online*, Reem Al Assil conseguiu mostrar ao mundo o que estava a acontecer no seu país e as ações desenvolvidas pelo regime sírio à época.

O próprio movimento da Primavera Árabe teve as suas raízes na *Deep Web*, bem como vários outros movimentos libertários que ocorreram nessa região do país. Utilizando o anonimato, seria impossível que reuniões entre membros desses grupos fossem denunciadas, e muitas situações passaram a ser denunciadas tal como muitos movimentos ativistas tomaram voz.

Além de movimentos de ativismo através da *Deep Web*, um outro fenómeno viria a surgir cimentado pelas mesmas bases: o jornalismo *online* ganhou um enorme impulso graças à *Deep Web*. Pelas mesmas razões, vários foram os acontecimentos divulgados em países que adotam a censura na *Internet*, os jornalistas passaram a adotar esta técnica para contornar os mecanismos de censura, e, assim, aumentar a sua rede de trabalho e divulgação.

4.1.2- WikiLeaks

Imagem 5- Logotipo da *WikiLeaks*

O *WikiLeaks* é uma organização sem fins lucrativos com o seu domínio *online* fundada pelo australiano Julian Assange, que organiza documentos e informações confidenciais postados por fontes anónimas. Os assuntos dos documentos postados são, na sua maioria, temas sensíveis, constrangedores e incriminatórios para grandes e poderosas organizações mundiais, como governos nacionais. Dado que as publicações do *WikiLeaks* poderão pôr em causa a segurança e bem estar dos seus autores, é recomendável (até pelo próprio *WikiLeaks*) que os autores garantam o seu anonimato, utilizando o *software Tor* por exemplo. Desta forma, o *WikiLeaks* pode garantir que as suas fontes não serão divulgadas, e que será extremamente difícil serem identificadas. Entre as mais importantes e polémicas divulgações destacam-se duas:

> O *WikiLeaks* divulgou em meados de 2010 cerca de 92 mil documentos de relatórios do período entre 2004 e 2009 dos serviços secretos do exército americano, que reportava à morte de milhares de civis inocentes durante a guerra do Afeganistão por parte dos militares norte-americanos. Nestes relatórios, foram descritos várias ações de abuso de autoridade, atentados aos direitos humanos e crimes de guerra.
>
> Em 2007, ficou célebre a publicação de um vídeo de um ataque de um helicóptero *Apache* norte-americano em Bagdad, Iraque, que vitimou 12 pessoas, entre as quais jornalistas e outros inocentes. Na mesma data, foi também publicado um documento de uma cópia do manual de instruções para o tratamento de prisioneiros na prisão de Guantánamo, Cuba. Neste documento estavam descritas atrocidades cometidas pelos funcionários norte-americanos da prisão aos prisioneiros.

As ações desenvolvidas pelo *WikiLeaks*, apesar de serem consideradas como ameaça por várias entidades (entre as quais o governo norte-americano, criador do *software Tor),* foram altamente valorizadas por várias instituições como a Amnistia

Internacional, e Julian Assange chegou inclusivamente a ser considerado para vencedor do prémio *Nobel* da paz pela criação do *WikiLeaks.*

4.2 Lado negativo (casos)

Tal como foi mencionado anteriormente, o anonimato *online* e o acesso à *Deep Web*, pode revelar consequências muito negativas se utilizados maliciosamente. O anonimato é uma ferramenta ideal para o crime, e o *Tor* é um veículo de promoção do mesmo. No presente capítulo serão enunciados exemplos de como o uso malicioso desta tecnologia pode resultar em criminalidade.

4.2.1- Silk Road

Silk Road é um *site* de mercado negro, mais conhecido por vender drogas, que opera na *Dark Web*. Como foi referido previamente, é necessário um *software*, como o *Tor*, para aceder a esta plataforma. Sendo um espaço em que as pessoas se "movimentam" de forma anónima, é extremamente complicado de identificá-las pelas autoridades, razão pelo qual recolhe tanto interesse pelos utilizadores. *Silk Road* foi lançado em fevereiro de 2011 e, inicialmente, havia um número limite de utilizadores, em que quem quisesse tornar-se membro teria de adquirir uma conta em leilões. Mais tarde, levantaram a restrição quanto ao número de utilizadores, bastando que os membros pagassem uma certa quantia inicial.

Acredita-se que o *Silk Road* fosse gerido por Ross Ulbritch, sob o pseudónimo "Dread Pirate Roberts", uma personagem fictícia do romance "*The Princess Bride*". Para além de Ulbritch, 2 administradores segundo os nomes de "*Variety Jones* e "*Smedley*" também geriam o *site*. O *site* ganhou uma grande notoriedade quando o *blog Gawker*, em 2011, publicou um artigo sobre ele, provocando um tremendo tráfego na plataforma. O Departamento de Justiça e a Agência de Combate às Drogas entraram em ação com o intuito de apagar o *site* mas sem sucesso. Em fevereiro de 2013, um traficante australiano tornou-se a primeira pessoa a ser detida por vender drogas no *Silk Road,* depois das autoridades intercetarem uma encomenda feita por ele pelo correio. Em dezembro desse ano, um neozelandês foi condenado a 2 anos e 4 meses de prisão após ter encomendado 15 gramas de metanfetaminas que tinha comprado no *Silk Road*.

No dia 2 de outubro de 2013, Ross Ulbritch é detido pelo *FBI* numa biblioteca em *San Francisco*, sob suspeitas de estar por trás do *Silk Road*. Ulbritch foi acusado de lavagem de dinheiro, *hacking*, conspiração sobre tráfico de narcóticos e tentativa de homicídio de 6 pessoas. Contudo, as autoridades acabaram por retirar esta última acusação por falta de provas. Antes do julgamento, Ulbritch terá escrito numa carta que o "*Silk Road* era suposto ser um espaço para que as pessoas se pudessem expressar livremente" e admitiu que cometeu um erro terrível que lhe arruinou a vida. A 29 de maio de 2015, foi condenado a 5 penas, entre elas duas perpétuas, sem a hipótese de fiança.

No final de 2014, havia cerca de 18 000 produtos listados pelos vendedores, em que cerca de 70% eram drogas, sobre várias categorias tais como estimulantes, psicadélicos, receitas médicas, ópio, *ecstasy*, dissociativos, *canábis* e esteróides. Cartas de condução falsas também se encontravam disponíveis para venda. Os termos e condições de uso impediam a venda de certos artigos, como pornografia infantil, cartões de crédito roubados, homicídios e todo o tipo de armas. Os compradores escreviam críticas num fórum associado ao *site*, onde davam as suas opiniões sobre os melhores e piores vendedores de droga no *Silk Road*.

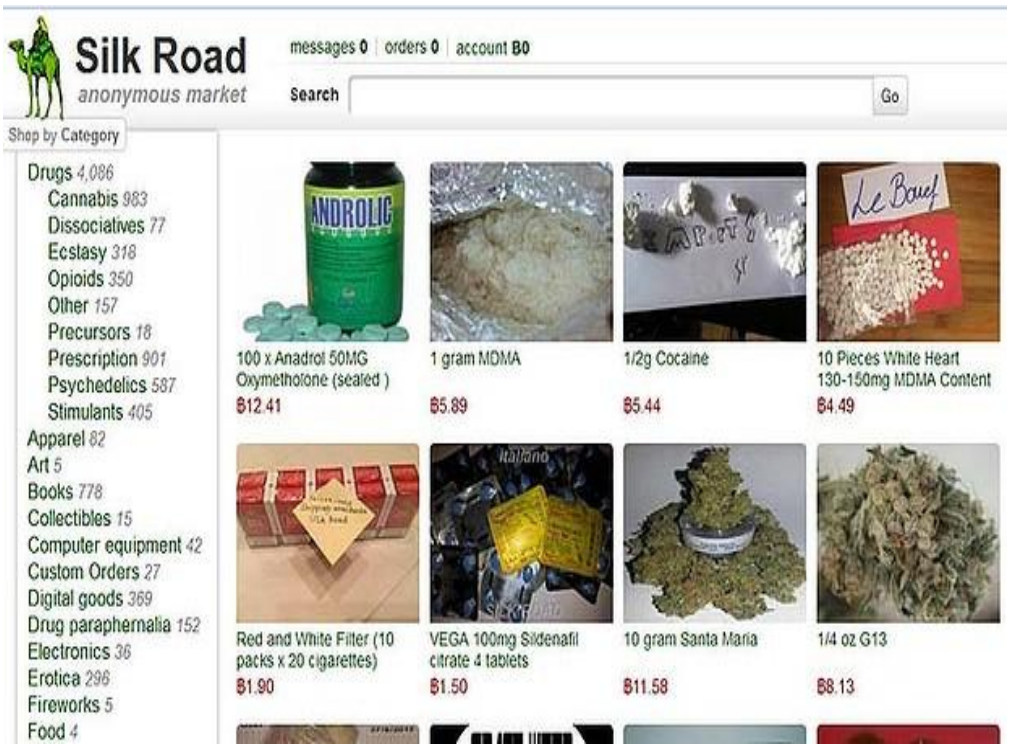

Imagem 6- *Silk Road*

As transações no *Silk Road* eram efetuadas por *Bitcoins*, e estima-se que as receitas provenientes dessas transações tenham atingido os 9 519 664 ฿, que corresponde a cerca de 1,2 biliões de dólares e, em comissões, 614 305 ฿, traduzindo-se em 79.8 milhões de dólares, envolvendo mais de 146 946 compradores e 3 877 vendedores. Segundo foi possível apurar, 30% das transações eram efetuadas para os Estados Unidos, 27% para paradeiro incerto, e as restantes dividiam-se por países como o Reino-Unido, Austrália, Alemanha, Canadá, Suécia, França, Rússia, Itália e Holanda. De seguida, é apresentado um esquema de como se efetua uma transação pelo *Silk Road*.

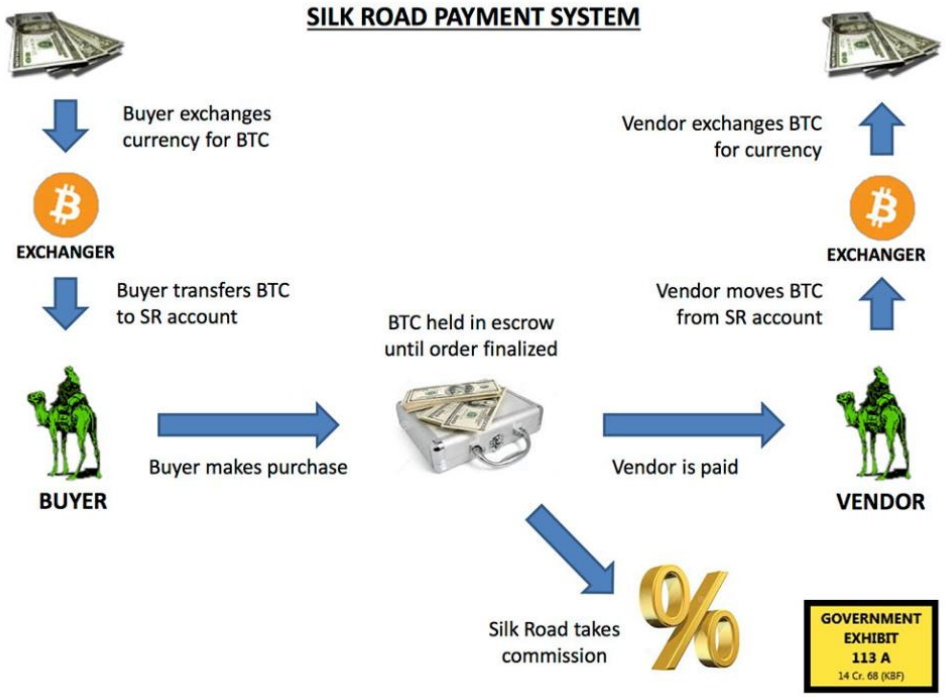

Imagem 6 – Forma de pagamento via *Silk Road*

Depois de ter sido encerrado aquando da detenção de Ross Ulbritch, o *Silk Road* foi reaberto a 6 de novembro de 2013 sob o nome de "*Silk Road* 2.0".

4.2.2- Sites similares

O *Black Market Reloaded* é um *website* existente na *Deep Web* onde se vende de tudo, desde drogas e armas a todo o tipo de pornografia e cartões de crédito roubados. Ao contrário do *Silk Road*, não apresenta qualquer tipo de restrições. A sua popularidade aumentou exponencialmente desde que o *Silk Road* foi fechado, contudo, o administrador do *Black Market Reloaded* revelou mais tarde que o *site* iria fechar devido às dificuldades em gerir o novo fluxo de utilizadores da plataforma.

Outro *site* dessa natureza é o "*The Farmer's Market*", mas não utiliza o sistema de *Bitcoins*, razão pela qual as transações são facilmente rastreáveis.

5. Algumas soluções

As questões que surgiram com o anonimato *online*, tendo em conta de se tratar de um tema que acarreta aspetos tanto positivos (combater e evitar a censura na internet) como negativos (crime online), foram tema de análise por parte de algumas entidades que sempre estiveram ligadas ao espaço cibernético quase desde a sua criação, e com vasta experiência no campo da segurança na *Internet*. Das soluções que foram apresentadas, destacam-se duas.

Eugene Kaspersky, *CEO* de uma empresa de segurança na *Internet* de seu nome *Kaspersky,* cujos produtos principais desenvolvidos são sistemas de antivírus, defende que na *Internet* é impossível atingir a privacidade sem segurança, e que navegar na *Internet* terá sempre sempre os seus riscos de invasão de privacidade. Tendo em conta a premissa, a solução encontrada passa por um balanço entre liberdade e segurança, bem como o anonimato e identificação constante. Kaspersky admite a criação de um "passaporte *online*" para cada utilizador que obriga à identificação dos dados do mesmo, em casos específicos como transações bancárias.

Outra solução estudada passa por melhorar a arquitetura da *Internet* e torná-la mais resistente a estas ameaças, através da encriptação. No entanto, a criptografia revela-se como uma técnica morosa e difícil de aplicar, tanto que até mesmo os utilizadores da técnica profissionalmente por vezes têm dificuldades. Além do mais, existe muito maior facilidade em encriptar uma mensagem do que a desencriptar a mesma, o que tornaria o sistema mais lento e ineficiente.

É possível concluir que qualquer solução apresentada possui falhas, e que nenhuma é perfeita. A solução deverá partir do princípio que é impossível tornar o sistema perfeitamente seguro e que não é, tão pouco, possível proteger todas as pessoas em todas as situações.

6. Debate e reflexão

A criação da *Internet* foi um fenómeno que abriu novas portas ao conhecimento e que aproximou as pessoas. O conhecimento e a informação está agora ao alcance de qualquer um, as fronteiras são um conceito cada vez mais vago, e a *Internet* tornou-se uma ferramenta transversal a qualquer geração e grupo social, como foi referido no capítulo da introdução, estamos a presenciar a revolução das novas TI.

No entanto, a sociedade apercebeu-se muito mais cedo das vantagens que a *Internet* oferecia do que os riscos que proporcionava. A *Internet* obrigou a que o conceito de "limites da privacidade" fosse repensado a partir do momento em que os utilizadores se aperceberam que é impossível usufruir das suas vantagens sem fazer algumas cedências.

Foi a dicotomia privacidade/segurança que ofereceu uma solução que, à época, parecia ideal. Todavia, é irónico observar como essa solução se tornou uma ameaça, mesmo para os próprios criadores da solução. Foi a *US Naval Research Lab* a criadora não só do conceito de *Darknet* e anonimato na *Internet*, como também do s*oftware Tor*, que tantos aspetos positivos e vantagens ofereceu ao mundo, no entanto, são os mesmos os autores de grandes ameaças e criadores de condições para o mercado negro e crime *online*.

Será impossível encontrar uma solução ideal- todas as soluções encontradas para resolver problemas que surgiram revelaram-se apenas ideais temporariamente pois mais tarde levantaram outros problemas. O balanço e equilíbrio deverá ser sempre o fator a ter em conta enquanto se lida com este problema, a segurança nunca será absolutamente garantida sem retirar benefícios à utilização da *Deep Web*.

Ainda assim, apesar da solução ter de passar necessariamente por este balanço, a paz na Internet não passa apenas pelos grandes agentes responsáveis pela mesma e sua segurança, mas também de uma mudança urgente da consciencialização da sociedade. A *Deep Web* oferece um novo mundo de conteúdos valiosos que se encontram perdidos, mas também conteúdo que a maioria das pessoas preferirá nem saber que existe e proporciona condições para a criminalidade, cabendo à sociedade adotar um comportamento responsável aquando da utilização da *Deep Web.* Os problemas que a *Deep Web* trouxe são em tudo semelhantes aos que já existem no mundo real, e assim terão de ser as soluções a encontrar.

7. Bibliografia

www.torproject.org

www.wikileaks.org

Apontamentos das aulas de Sociologia das Novas Tecnologias de Informação do professor António Brandão Moniz, do ano letivo 2015/2016

Documentário da BBC "*Inside the Dark Web*", 2014

https://www.amnesty.org.uk/blogs/campaigns/syrian-activist-reem-al-assil-opens-2014-amnesty-international-uk-conference

TEDx Talks: *The Dark Web*- Alan Pearce

TEDx Talks: *The Tor Project, protecting online anonymity*- Jacob Appelbaum

http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/

www.darkwebnews.com

www.bitcoin.org